

Weekly Report

2019.06.10-2019.06.16

Doing & done

Mon, 8h

在玉泉上课

☒ 《机器学习》

组会报告

☒ 精读完报告的文章，并完成PPT的前半部分。（1/2）

Tue, 8h

阅读文献

☒ 《Privacy Preserving Machine learning: Threats and Solutions》：这篇文章作为一篇综述，讲了机器学习和基础知识以及隐私保护和同态加密的一系列经典方法，介绍了机器学习中数据安全方面遇到的各类挑战。为我idea的技术路线提供了一个比较全面的参考。

组会报告

☒ 继续阅读文章，完成报告PPT。（2/2）

Wed, 8h

在玉泉上课

☒ 《高级操作系统》课堂展示

组会报告

☒ 准备明天组会报告展示，排练

Thu, 8h

组会报告

☒ 准备组会报告展示，修改PPT

可解释机器学习

☒ 学习刘世霞老师的《可解释机器学习可视化》的讲座，启发：

- 联邦学习的鲁棒性？例如对攻击client的噪声的反应。结合已有的检测算法，思考可视化方式，参考以下论文：

Analyzing the Noise Robustness of Deep Neural Networks

Mengchen Liu, Shixia Liu, Hang Su, Kelei Cao, Jun Zhu

datapath extraction

- Hybrid visualization
 - Rectangle packing
 - Matrix visualization
 - Biclustering-based edge bundling

Fri, 8h

在玉泉上课

☒ 《机器学习》

tensorflow_federate

☒ 配置环境，运行tff的demo，验证上周提出的初步想法。

Work plan

- 继续本周完成的进度，对tensorflow_federate的结果进行分析和处理，观察投影后的结果。
- 继续阅读深度学习可解释性、隐私保护机器学习相关论文，思考其他idea的可行性。